3-03082-KS

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－61277

(43)公開日　平成10年(1998)３月３日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｅ０５Ｂ	49/00			Ｅ０５Ｂ	49/00	Ｋ	
Ｂ６０Ｒ	25/00	６０６		Ｂ６０Ｒ	25/00	６０６	
Ｅ０５Ｂ	47/00			Ｅ０５Ｂ	47/00	Ｕ	
	65/19				65/19	Ｂ	
	65/20				65/20		

審査請求　未請求　請求項の数６　ＯＬ　（全６頁）　最終頁に続く

(21)出願番号　特願平8－222044

(22)出願日　平成８年(1996)８月23日

(71)出願人　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地

(72)発明者　中野　彰夫
愛知県刈谷市昭和町１丁目１番地　日本電装株式会社内

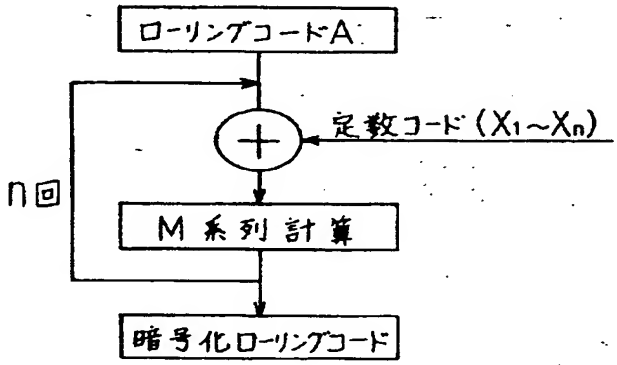
(74)代理人　弁理士　碓氷　裕彦

(54)【発明の名称】　遠隔操作装置

(57)【要約】

【課題】　設計者といえども送信コードの解読ができないようにすること。

【解決手段】　ローリングコード変更テーブル中の定数コードＸとローリングコードＡとの排他的論理和の演算、および周知のＭ系列演算をｎ回繰り返しにより、ローリングコードＡが暗号化され、暗号化ローリングコードが生成される。なお、ｋ回目の排他的論理和の演算の際には、車両固有のキーコードが定数コードX_kとして用いられることになるので、ｋ回目の排他的論理和の演算の方法は車両毎に異なることになり、しいては、暗号化の方法が車両毎に異なることになる。また、キーコードは車両の製造工程においてＥＥＰＲＯＭ１９に書込まれるようになっているので、キーコードを製造工程まで秘密にしておけば、設計者であっても、ローリングコードＡの暗号化は見破られることない。



【特許請求の範囲】
【請求項１】　固有の識別情報がコード化されたＩＤコードと、このＩＤコードを暗号化するために用いられるローリングコードとの２つのコードを含む送信コードを送信する送信機と、前記送信機から送信された前記送信コードを受信して、この送信コードから前記ＩＤコードを復元し、復元されたＩＤコードに基づいて制御の対象を作動させる指令を出力する受信機とを備えた遠隔操作装置において、
前記送信機は、
各々の装置固有に定められたキーコードを格納した格納手段と、
前記キーコードに基づいて前記ローリングコードを暗号化して暗号化ローリングコードを生成する生成手段と、前記暗号化ローリングコードを用いて前記ＩＤコードを暗号化する暗号化手段とを備えることを特徴とする遠隔操作装置。
【請求項２】　前記送信機内に互いに異なる定数コードが設定されたローリングコード変更テーブルを備え、前記生成手段は、前記ローリングコードと前記ローリングコード変更テーブルに設定された前記定数コードとを論理演算することにより暗号化ローリングコードを生成するものであることを特徴とする請求項１記載の遠隔操作装置。
【請求項３】　前記生成手段は、前記ローリングコードと前記定数コードとを論理演算した後に、Ｍ系列計算を行うことにより暗号化ローリングコードを生成するものであることを特徴とする請求項２記載の遠隔操作装置。
【請求項４】　前記生成手段は、前記論理演算と前記Ｍ系列計算を複数回繰り返して行うことにより、暗号化ローリングコードを生成するものであることを特徴とする請求項３記載の遠隔操作装置。
【請求項５】　前記格納手段は不揮発性記憶媒体を含み、前記キーコードは装置の製造工程において前記不揮発性記憶媒体に記憶されるものであることを特徴とする請求項２記載の遠隔操作装置。
【請求項６】　前記キーコードは、前記不揮発性記憶媒体から読み出され、前記ローリングコード変更テーブルに設定された定数コードの少なくとも１つに設定されるものであることを特徴とする請求項５記載の遠隔操作装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、車両のワイヤレスドアロック制御装置等に用いられる遠隔操作装置に関するものである。
【０００２】
【従来の技術】従来、車両のワイヤレスドアロック制御装置に採用されるような遠隔操作装置では、不正防止の観点から、送信機から送信される送信コードを解読されないように暗号化することがなされている。例えば、特開平８－１０２９８２号公報に開示された装置では、送信コードが送信される毎に所定の順序で変更されるローリングコードを用いて送信コードを暗号化している。
【０００３】
【発明が解決しようとする課題】しかしながら、上記公報に開示された装置では、ローリングコードの変更順序は予め設定されているものであるため、この変更順序を設定した者、すなわち設計者であれば暗号化された送信コードの解読が可能であり、十分な暗号化がなされているとは言えなかった。
【０００４】そこで本発明は上記問題点に鑑みてなされたものであり、解読の難しさを向上し、設計者といえども送信コードの解読を困難とした遠隔操作装置を提供することを目的とするものである。
【０００５】
【課題を解決するための手段】上記目的を達成するため請求項１記載の発明では、送信機は、各々の装置固有に定められたキーコードに基づいてローリングコードを暗号化して暗号化ローリングコードを生成し、暗号化ローリングコードを用いてＩＤコードを暗号化する。よって、装置固有に定められたキーコードさえ秘密にしておけば、暗号化ローリングコード生成のアルゴリズムを設定したものであっても、ローリングコードの暗号化の解読は困難となるので、送信コードの解読の難かしさが向上し、ユーザ以外の不正な使用を防止することができる。
【０００６】請求項４記載の発明では、論理演算とＭ系列計算を複数回繰り返して行うことにより暗号化ローリングコードを生成しているので、一層ローリングコードの暗号化の解読は困難なものとなる。請求項５記載の発明では、キーコードは、装置の製造工程において不揮発性記憶媒体に記憶されるようにしているので、装置の製造工程までキーコードを秘密にしておく、あるいは製造工程でランダムにキーコードを設定すれば、ローリングコードの暗号化は解読されることはない。
【０００７】
【発明の実施の形態】以下、本発明の実施の形態を図面を用いて説明する。
〔第１の実施形態〕図１は、本発明の遠隔操作装置を車両用のワイヤレスドアロック制御を行う装置に採用した際の第１の実施形態の構成を示すブロック図である。
【０００８】図１において、１は送信機であり、この送信機１は、それぞれ異なった機能（例えば、ドアロック、トランクの開閉、シートポジションの設定等）を遠隔作動させるためのスイッチ１２－１，１２－２，…，１２－ｎが設けられており、そのスイッチ操作はマイクロプロセッサ１１に入力されるように構成されている。このマイクロプロセッサ１１は、ＥＥＰＲＯＭ１９が接続されており、このＥＥＰＲＯＭ１９には、送信機１固

有のＩＤコードＡと、送信コードが送信される毎に所定の順序で変化するローリングコードＡと、車両固有のキーコードとが記憶されている。これらのＩＤコードＡ、ローリングコードＡ、およびキーコードは、車両の製造工程においてＥＥＰＲＯＭ１９に記憶させるものである。また、マイクロプロセッサ１１中には、ローリングコードＡを暗号化するためのローリングコード変更テーブルと、送信コード生成のための情報とがアルゴリズムとして記憶されている。ローリングコード変更テーブルは、図３に示すように構成されている。図３中、x_1 番地～x_n 番地には、各々異なるｊビットからなる定数コードX_1 ～X_n が設定されている。このうち、x_k 番地（$1 \leqq k \leqq n$）には、ＥＥＰＲＯＭ１９から車両固有のキーコードが読み出され、定数コードX_k として設定されるようになっている。さらに、マイクロプロセッサ１１には、発信回路１４及びＦＭ変調回路１５が接続されており、マイクロプロセッサ１１にて生成された送信コードをＦＭ変調して微弱電波として放射するように構成されている。

【０００９】一方、受信機２には、送信機１から放射された微弱電波を復調する受信回路が設けられており、この受信回路は高周波増幅回路２５、局部発振器２４、ミキサ回路２６、中間周波増幅回路２７、復調回路２８によって構成され、その復調された出力信号がマイクロプロセッサ２１に入力されるように構成されている。なお、このマイクロプロセッサ２１は、予め定められた所定の処理に基づいて、復調された出力信号からＩＤコードＡとローリングコードＡを復元する。また、マイクロプロセッサ２１にはＥＥＰＲＯＭ２９が接続されており、このＥＥＰＲＯＭ２９は受信機２固有のＩＤコードＢと、前回受信した送信コードに含まれていたローリングコードＡに対応したローリングコードＢと、車両固有のキーコードとが記憶されている。また、マイクロプロセッサ２１中には、ローリングコードＡを復元するためのローリングコード変更テーブル（図３と同じ）と、出力信号からＩＤコードＡとローリングコードＡを復元するのための情報とがアルゴリズムとして記憶されている。そして、マイクロプロセッサ２１には、駆動回路２３－１，２３－２，…，２３－ｎを介して、制御対象となる３－１，３－２，…，３－ｎ（例えば、ドアロック、トランクの開閉、シートポジションの設定等を行うアクチュエーター）が接続されており、この制御対象となる３－１，３－２，…，３－ｎはマイクロプロセッサ２１からの信号に応じて作動するように構成されている。

【００１０】次に、上記構成の送信機１及び受信機２の動作を図２に示すフローチャートに基づき説明する。なお、このフローチャートはそれぞれ送信機１、受信機２に設けられたマイクロプロセッサ１１、２１により実行される処理を示す。まず、送信機１の動作を説明する。ステップ１０にて、スイッチ１２－１～１２－ｎのいずれかが操作されたと判断するまで待機し、スイッチが操作されたと判断した時点でステップ２０に移行する。ステップ２０にて、ローリングコードＡの更新を行う。このローリングコードＡはｊビットからなる変数で、送信が行われる毎に＋１変化するものとする。なお、送信が行われる毎に＋１変化するとしているがこれに限らず、所定の規則に従って変化するものであればよい。

【００１１】次に、ステップ３０にて、ローリングコード変更テーブルを用いてローリングコードＡを暗号化することにより暗号化ローリングコードを生成する。この暗号化ローリングコードの生成方法を図３、および図４を用いて説明する。まず、図３に示すローリングコード変更テーブル中のx_1 番地の定数コードX_1 とローリングコードＡとの排他的論理和の演算を行う。次に、周知のＭ系列演算を行う。その後、x_2 番地以降の定数コードＸを用いた排他的論理和の演算とＭ系列計算をｎ回繰り返す。この排他的論理和の演算とＭ系列計算の繰り返しにより、ローリングコードＡが暗号化され、暗号化ローリングコードが生成される。なお、ｋ回目の排他的論理和の演算の際には、車両固有のキーコードが定数コードX_k として用いられることになるので、ｋ回目の排他的論理和の演算の方法は車両毎に異なることになり、しいては、暗号化の方法が車両毎に異なることになる。また、キーコードは車両の製造工程においてＥＥＰＲＯＭ１９に書込まれるようになっているので、キーコードを製造工程まで秘密にしておく、あるいは製造工程でランダムにキーコードを設定すれば、図４に示すロジックを考えた設計者であっても、ローリングコードＡの暗号化は解読されることはない。

【００１２】次に、ステップ４０にて、暗号化ローリングコード、ＥＥＰＲ０Ｍ１９に記憶されているＩＤコードＡ、および機能コードとを用いて送信コードを生成する。機能コードとは、制御対象となる３－１，３－２，…，３－ｎを作動させるためのコードである。そして、ステップ５０にて、ステップ４０で生成された送信コードをＦＭ変調回路１５に出力する。これにより、送信コードはＦＭ変調されて微弱電波として送信機１外部に放射される。送信コード送信する。なお、送信コードの生成については、前述した特開平８－１０２９８２号公報に詳しいのでそちらを参照されたい。

【００１３】以上の一連のステップは、操作スイッチが一回押された場合の送信機１側の処理であって、再び操作スイッチが押された場合は、ステップ２０～５０の処理が再度実行され、この場合、ローリングコードは変更されることになる。次に、受信機２の動作を説明する。ステップ１１０にて、送信機１からの送信コードが受信されるまで待機し、送信コードが受信された時点でステップ１２０に移行する。ステップ１２０では、送信コードからＩＤコードＡとローリングコードＡとを復元す

る。

【００１４】次に、ステップ１３０にて、ＥＥＰＲＯＭ２９に記憶されているＩＤコードＢとステップ１２０で復元された送信コードのＩＤコードＡとが一致するか否かを判定する。一致すればステップ１５０に移行し、一致しなければステップ１１０にて待機状態となる。さらに、ステップ１４０にて、ステップ１２０で復元されたローリングコードＡと、ＥＥＰＲＯＭ２９に記憶されているローリングコードＢとを比較し、復元されたローリングコードＡがローリングコードＢに対し所定の範囲内にあるか否かを判定する。範囲内であれば、ローリングコードは正しいとしてステップ１５０に移行し、範囲外であればステップ１１０にて待機状態となる。このとき、送信機１の送信コードが受信機２側で毎回受信されるのであれば、受信機側で比較判定するローリングコードＡは、ローリングコードＢの値＋１に限定してもよい。しかしながら、送信機１が操作されても受信機側で受信されない場合（いわゆる送信機１のカラ打ち）、送信機１のローリングコードＡのみが更新されるため、この場合にも対応できるように許容範囲を定めている。例えば、送信コードから復元したローリングコードＡの値r_i、ＥＥＰＲＯＭ２９に記憶されているローリングコードＢの値r_{i-1}として、”$r_{i-1}+1 \leqq r_i \leqq r_{i-1}+\alpha$”（$\alpha$は任意の自然数）であればローリングコードＡは正常であると判定する。

【００１５】次に、ステップ１５０にて、送信コードから復元したローリングコードＡをＥＥＰＲＯＭ２９にローリングコードＢとして記憶することにより、ローリングコードＢを更新する。これによって、送信機１のカラ打ちにより送信機１のローリングコードＡのみが更新され、送信機１と受信機２とに設定されるローリングコードに差が生じたとしても、受信機２が送信コードを受信した場合には、送信コードから復元したローリングコードＡでローリングコードＢを更新するので、送信コード受信後のローリングコードＡとローリングコードＢは一致することになる。

【００１６】さらに、ステップ１６０にて、送信コードに設定されていた機能コードに対応して、駆動回路２３－１，２３－２，…，２３－ｎを介して、制御対象となる３－１，３－２，…，３－ｎを作動させる。なお、この実施形態においては、ＥＥＰＲＯＭ１９、およびローリングコード変更テーブルのx_k番地が格納手段に相当し、図２のステップ３０の処理が生成手段に相当し、図２のステップ４０の処理が暗号化手段に相当する。

【００１７】〔他の実施形態〕第１の実施形態では、ローリングコードの暗号化処理は、１回の排他的論理和の演算と１回のＭ系列計算を１セットとしているが、図５に示すように、１回の排他的論理和の演算と２回のＭ系列計算を１セットとしてしても良いし、図６に示すように、２回の排他的論理和の演算と２回のＭ系列計算を１セットとしてしても良い。さらに、図７、８に示すように、１回目のＭ系列計算が終了した後に、ローリングコードを構成しているｊビットの信号の前半部分と後半部分とを入れ替えるようにしても良い。図５～図８の暗号化処理を採用することによって、暗号化ローリングコードの解読が一層困難なものとなる。

【００１８】第１の実施形態では、ＥＥＰＲＯＭ１９，２９は、マイクロプロセッサ１１，１２と別体に構成しているが、マイクロプロセッサ１１，１２に内蔵しても良い。また、第１の実施形態では、キーコードはローリングコード変更テーブルのx_k番地のみに設定されていたが、複数の番地に設定するようにしても良い。さらに第１の実施形態では、幾つかの機能を作動させる構成としたが、機能を単一のものにすることによって、機能ビットのない応用例を実現することもできる。

【図面の簡単な説明】

【図１】本発明の実施形態の構成を示すブロック図である。

【図２】図１に示す送信機、受信機の動作を表すフローチャートである。

【図３】ローリングコードＡを暗号化するためのローリングコード変更テーブルである。

【図４】第１の実施形態におけるローリングコードＡを暗号化するためのロジックを説明するための図である。

【図５】他の実施形態におけるローリングコードＡを暗号化するためのロジックを説明するための図である。

【図６】他の実施形態におけるローリングコードＡを暗号化するためのロジックを説明するための図である。

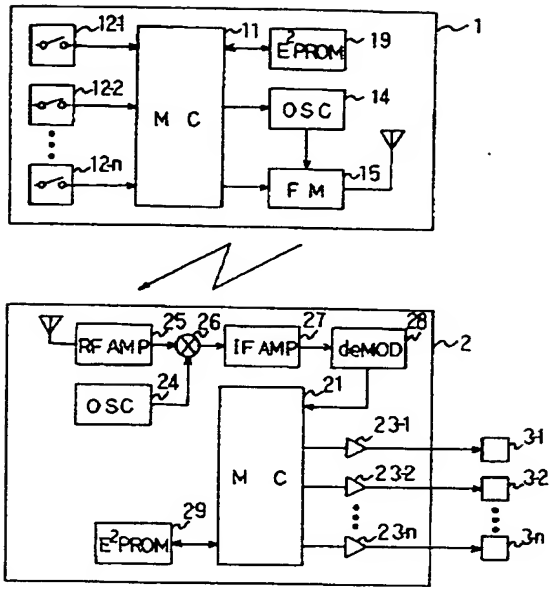
【図７】他の実施形態におけるローリングコードＡを暗号化するためのロジックを説明するための図である。

【図８】他の実施形態におけるローリングコードＡを暗号化するためのロジックを説明するための図である。

【符号の説明】

１　送信機
２　受信機
３　アクチュエータ
１１　マイクロプロセッサ
２１　マイクロプロセッサ

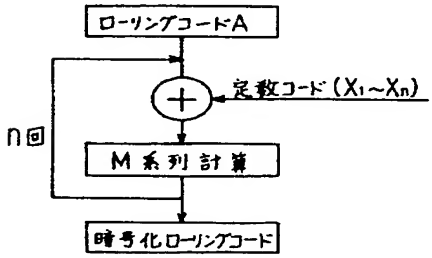
【図１】



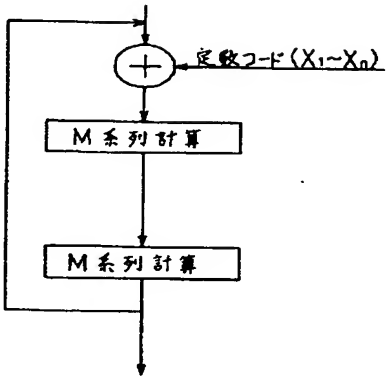
【図３】

番地	定数コード（Jビット）	
X_1	定数コード X_1	
X_2	定数コード X_2	
X_k	定数コード X_3	← キーコード
X_n	定数コード X_n	

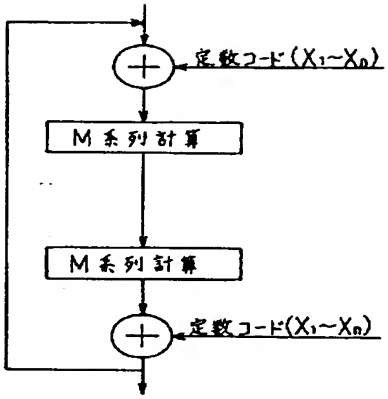
【図４】



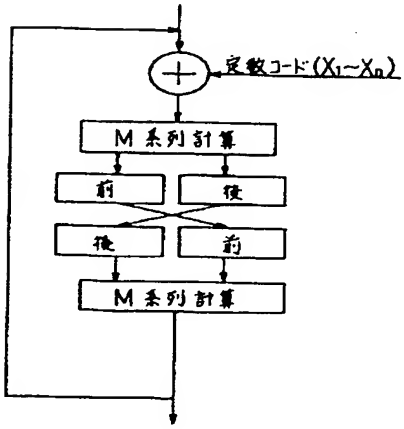
【図５】



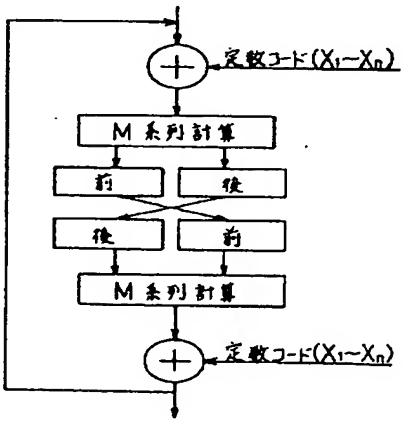
【図６】



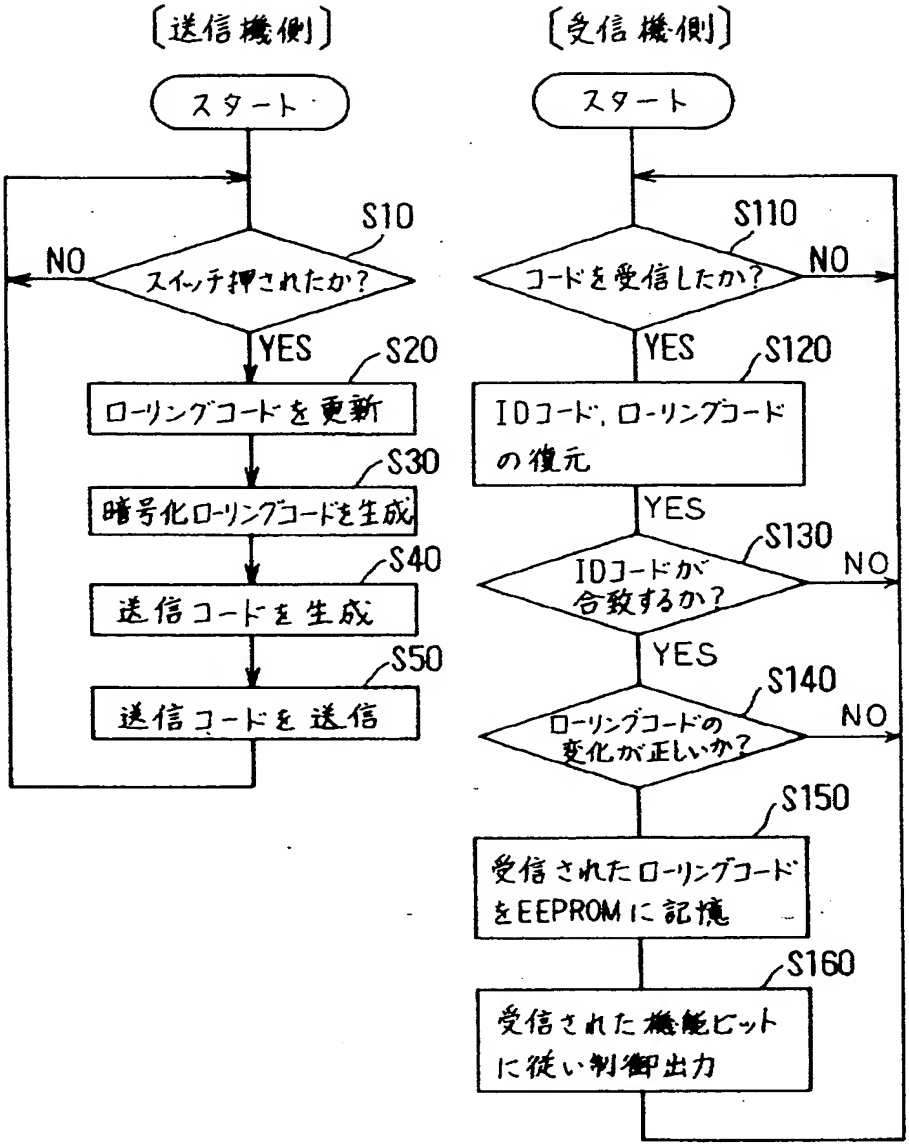
【図７】



【図８】



【図２】



フロントページの続き

(51) Int. Cl. 6		識別記号	庁内整理番号	FI		技術表示箇所
H04Q	9/00	301		H04Q	9/00	301B
		311				311N